UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA	:	
- v. -	:	S1 24 Cr. 293 (JGLC)
ANTON PERAIRE-BUENO, and JAMES PERAIRE-BUENO,	:	
Defendants.	:	

THE GOVERNMENT'S OPPOSITION TO DEFENDANTS' MOTION TO COMPEL PURPORTED EXPERT DISCLOSURES FROM PERCIPIENT WITNESSES

JAY CLAYTON
United States Attorney

Rushmi Bhaskaran
Jerry Fang
Danielle Kudla
Assistant United States Attorneys

- *Of Counsel* -

TABLE OF CONTENTS

PRELIMINARY STATEMENT

The Government submits this memorandum in opposition to defendants Anton Peraire-Bueno and James Peraire-Bueno's motion to compel purported expert disclosures (the "Motion to Compel," *see* Dkt. 103). That Motion takes the extraordinary position that the Government's lay witnesses—including a victim of the defendant's alleged fraud, a cooperating witness, and a witness from the company whose software vulnerability was exploited by the defendants to commit the charged crimes—are expert witnesses whose testimony is subject to the strict gatekeeping rules of Rule 16(a)(1)(G) and *Daubert v. Merrell Dow Pharmaceuticals*, 509 U.S. 579 (1993). In essence, the defense would require these witnesses to write out their anticipated testimony in advance, sign that description of their testimony, and to be subject to potential motion practice and hearings to bar their testimony based on their qualifications and credentials. That position would lead to absurd results and should be rejected. While this case—like so many other fraud prosecutions in this District—involves technical facts, that does not transform victim, cooperating witness, and other lay witness testimony that is well within their personal knowledge and rationally based on their own perceptions into expert testimony. The Motion should be denied.

Furthermore, the defendants' argument that they are unable to make their own expert disclosures without the disclosures that the Motion seeks is unsupported by the law or the record in this case. As an initial matter, there was no deficiency in the Government's expert disclosures, and therefore no basis for the defense to withhold their own expert disclosures. Here, the Government timely and thoroughly noticed one expert witness regarding cryptocurrency tracing, and as a courtesy, also provided the defense with a description of several other witnesses it intends to call at trial. Moreover, the Government is not required to present expert testimony in any given case, even where sophisticated matters are concerned. As in so many cases in this District, the

Government can prove its case-in-chief without expert testimony. For this reason, the defendants are also wrong that Rule 16 requires the defendants only to disclose experts that are "responsive" to a particular Government expert. Defendants commonly notice potential experts even in cases where the Government does not seek to offer any expert testimony. Finally, the defendants' argument is meritless for yet another reason: the defendants have more than sufficient information to notice any experts they seek to call for their own case-in-chief because the Superseding Indictment, the extensive Rule 16 discovery in this case, and the Government's further descriptions of the underlying conduct at oral argument provide a detailed account of the alleged fraud, including its technical execution. The Court should order the defendants to promptly comply with their legal obligation to notice any experts they intend to call in their case-in-chief.

RELEVANT BACKGROUND

One June 27, 2025, the Government provided Rule 16(a)(1)(G) notice of its intent to offer at trial the testimony of Chris Hoffmeister, who is a cryptocurrency and financial crimes specialist at TRM Labs, Inc., regarding cryptocurrency tracing analyses performed in connection with this case.[1] A copy of the Government's expert notice for Mr. Hoffmeister and the related cover letter to the defense is attached hereto as Exhibit A (under seal). In addition to providing expert notice consistent with the Court-ordered schedule, the Government also notified the defendants that the Government intends to offer percipient testimony from a cooperating witness ("CW-1"), a representative from Flashbots (the "Flashbots Representative"), and a victim trader ("Victim-1") concerning the April 2, 2023 exploit (the "Exploit"), and provided the names of those witnesses to

[1] The defendants' motion to compel does not challenge the adequacy of the Government's expert notice for Mr. Hoffmeister. Similarly, the defendants' motion does not dispute that the testimony of certain law enforcement analysts who extracted electronic devices seized from the defendants can be offered as lay testimony, not expert testimony subject to the strictures of Rule 702.

the defense.[2] The defendants now move to compel the Government to make expert disclosures under Rule 16(a)(1)(G) with respect to these percipient witnesses.

To assist the Court in assessing the instant motion, the Government provides the following additional information regarding the scope of the anticipated testimony of these witnesses.[3]

A. Victim-1

Victim-1 is the CEO of a quantitative trading firm that was defrauded of more than $13 million worth of cryptocurrency on the day of the Exploit. To explain the events leading up to this fraud, Victim-1 will provide necessary background and terms for the jury to understand the cryptocurrency trading that Victim-1's was engaged in when the Exploit happened. For example, Victim-1 will explain that, prior to the Exploit, Victim-1's trading firm owned and controlled trading bots (the "MEV Bots") that identify potential profitable trading opportunities based on publicly available trading data in the mempool. Victim-1 will explain how these trades take place in bundles of transactions: (1) the Victim-1's first trade, to buy the same token as the potentially profitable trade identified in the mempool ("Trade-1"); (2) the mempool transaction ("Trade-2"), which increases the price of the token the MEV Bots bought in Trade-1; and (3) Victim-1's sell transaction, which makes a profit by the increased price caused by Trade-2. Victim-1 will further

[2] While the Government noted that it may call additional witnesses whose testimony is similarly technical in nature in its letter to the defense, the Government has not identified any such likely witnesses at this time. Should the Government identify any such additional witnesses in the course of its trial preparations, the Government will disclose such witnesses to the defense in advance of trial.

[3] These summaries are not a complete recitation of these witnesses' testimony, but instead set forth the expected general contours of their testimony, and how their testimony is based on that which they directly observed. The Government will not necessarily elicit all of the testimony described herein, and the Government reserves the right to elicit testimony about additional topics that are covered by Rules 602 and 701, as the Government continues to prepare for trial.

explain that Victim-1 chose to use the MEV-Boost trading system to effectuate this trading strategy based on Victim-1's understanding that the MEV-Boost system provided certainty that the proposed bundles would be published to the chain as originally ordered and structured, or not at all.

Victim-1 will testify about how he learned that his cryptocurrency was stolen, and steps Victim-1 took to investigate the fraud. Based on Victim-1's investigation, Victim-1 learned that, during the Exploit, his MEV Bots proposed a bundle of transactions, but only the first transaction (*i.e.*, Trade-1 described above) went through successfully. However, Victim-1 learned that the second transaction (which caused the MEV Bots to trade in the first place) had been replaced before the block was published. Victim-1 will explain that he did not believe that such an alteration to his proposed bundle could happen because he was using the MEV-Boost system and relying on its specific features. In addition, based on his own investigation, Victim-1 learned that, for months, a particular user(s) in the Ethereum system had learned Victim-1's MEV Bots trading strategy by proposing particular trades in the mempool to cause the MEV Bots to trade.

Victim-1 will further describe his efforts to get Victim-1 money back, including his communications with the individuals he believed stole his money (the defendants).

B. CW-1

CW-1, the defendants' former employee, worked with the defendants on the Exploit and its aftermath. Through his communications with the defendants, CW-1 became familiar with the MEV-Boost system; the plans for the Exploit; how the Exploit was in fact executed; and how the proceeds from the Exploit were transferred into fiat currency.

CW-1 learned about the Exploit from the defendants in late 2022, as reflected in CW-1's contemporaneous notes. Among other things, these notes include a summary—reflecting

statements from the defendants—on their understanding of how the MEV-Boost system is supposed to work. For example, the notes contain the following description of the MEV-Boost system: "MEV-boost propose builder separation. Validators never see the blocks. . . validaotrs [sic] sign hashes and flashbots proagate block. validators don't see block until after it's done[.]" *See* Exhibit B (under seal). The contemporaneous notes further reflect that at the time the defendants' understanding that the Victim Traders and Flashbots would be upset with their actions: "tell nobody outside of ppl working on it. bigger concern is don't want targets on our back[.]" *Id*.

In the months leading up to the Exploit, CW-1 learned more details about the defendants' plans and sought out the defendants for answers on how the Exploit would take place, including how the MEV-Boost system was designed to operate. Some of these communications took place over Slack. In one such exchange with CW-1, Anton Peraire-Bueno described the MEV-Boost system, explaining that the "relay basically custodies this block." *See* Exhibit C (under seal). Anton then explained that, only after the validator signs the header does the Relay release the unblinded block with the private transaction data to the validator: "The validator signs this header, and sends this to the relay. They relay then. . .returns the UnBlindedBlock directly to us as an HTTP response[.]" *Id*. Anton also explained that, after the validator signs the header, the relay simultaneously sends the proposed block to the Ethereum nodes so the proposed block becomes part of the blockchain: "The relay then. . .starts propagating the UnBlindedBlock." *Id*.

Based on his work leading up to the Exploit and CW-1's communications with the defendants, CW-1 will describe how CW-1 worked with the defendants to target particular cryptocurrency traders. Once these traders were selected, CW-1, at the defendants' direction, used lure transactions to learn the trading behavior of these traders. In addition, CW-1 will further explain, based on CW-1's communications with the defendants, that the defendants identified a

coding vulnerability in the MEV-Boost software and decided to use the False Signature to carry out the Exploit to ensure its success.

CW-1 will also testify about his communications with the defendants in the aftermath of the Exploit. CW-1 will testify about how and why the defendants ultimately moved and converted the Exploit proceeds into fiat currency.

C. The Flashbots Representative

The Flashbots Representative learned on or about April 3, 2023 that there was a vulnerability in the MEV-Boost software that the Flashbots Representative was responsible for overseeing, and that the software vulnerability was exploited.

Flashbots is a research and development organization that developed the open-source MEV-Boost software, and the Flashbots Representative oversaw the development, testing, and implementation of MEV-Boost prior to the Exploit. Based on the Flashbots Representative's participation in Flashbots' investigation of the Exploit and his personal knowledge of how MEV-Boost was designed to function, the Flashbots Representative will describe that, through the Exploit, the relay released private transaction data to a validator when it was not designed to do so, which then allowed the validator to see and to change the contents of the proposed block at issue, contrary to the way that Flashbots had designed the MEV-Boost software. After the Exploit, the Flashbots Representative was directly involved with Flashbots' efforts to identify what had occurred and remediate the software vulnerability, and the Flashbots Representative also participated in post-hoc communications with the perpetrators about the Exploit.

The Government expects that the Flashbots Representative will explain how he learned of the Exploit, the steps that the Flashbots Representative and others (including other Flashbots employees and Ethereum network stakeholders) took to determine what had occurred, and what

he ultimately learned about how the Exploit was perpetrated. For example, the Government expects that the Flashbots Representative will describe how he learned about the False Signature and why it mattered to Flashbots, including the fact that the validator for the subject block had altered the parent and state roots of the blockheader before returning the signed (but invalid) blockheader to the relay, which enabled the validator to receive the private transaction data from the relay and propose an altered (but valid) block that was ultimately published. The Flashbots Representative will also describe the magnitude, urgency, and importance of the Exploit to Flashbots.

To place these events in context, the Flashbots Representative will explain that the Flashbots Representative and his colleagues designed the MEV-Boost software to enable anyone to participate competitively in the Ethereum consensus and realize the economic benefits of MEV, regardless of their size, sophistication, or resources. Prior to the advent of MEV-Boost, an Ethereum validator (also known as a proposer) had the dual roles of selecting the most profitable transaction to include in the next block, and also proposing the next block. However, the resource-intensive nature of selecting the most profitable transactions to include in the next block created higher barriers to entry by centralizing those that could construct economically competitive blocks to larger, more sophisticated, and well-resourced validators, leading to market inefficiencies. Thus, to lower barriers to entry and enable anyone to participate in the Ethereum consensus in a competitive way and gain the economic benefits from participating as a validator, the Flashbots Representative designed the MEV-Boost software to separate the dual roles of building a block (*i.e.*, selecting the transactions in the block) and validating the block, allowing parties to participate as validators so long as they "staked" a certain amount of Ether.

However, to address the lack of trust between block builders and validators who may be

unknown to each other (*e.g.*, a block builder may not trust that a validator will not unbundle the block or change the precise ordering of the block), the Flashbots Representative's team included a feature in the MEV-Boost software: a relay to act as an intermediary between a block builder and a validator. The Flashbots Representative's team designed the MEV-Boost software to permit the following steps: (i) the block builder orders a block and sends it to the relay; (ii) the validator asks the relay for the highest-value blockheader; (iii) the relay sends the blockheader without transaction contents to the validator; and (iv) the validator commits to publishing the block as structured by digitally signing the blockheader that is sent to the relay, after which the block is published to the Ethereum network.

The Flashbots Representative will explain what information the blockheader includes under the MEV-Boost software. For example, the Flashbots Representative will explain that the blockheader contains, among other things, a "parent root" and a "state root," which are fields in the blockheader that are pre-populated with a string of alphanumeric characters that act as unique identifiers for the proposed block and the preceding block. In addition, the Flashbots Representative will explain that after the Exploit, Flashbots Representative learned that the relay could be tricked into unintentionally releasing a block's private transaction contents to the validator, because the relay only checked to confirm that the validator that signed the blockheader was the validator that was selected to propose the next block—in other words, the relay did not check to confirm that the other fields of the blockheader, including the parent root or the state root, were valid.

The Flashbots Representative will describe that the way that the MEV-Boost software is designed to work—including the MEV-Boost architecture and the roles and interaction of the different MEV-Boost participants—is set forth on various online repositories that are open to the

public, including a "read-me" that accompanies the MEV-Boost software and user guides that are available on Flashbots's website, which the Flashbots Representative reviewed as part of his duties as the product lead responsible for MEV-Boost. The evidence will show that this information, published by Flashbots, was publicly available to MEV-Boost users and others prior to the Exploit.

ARGUMENT

I. The Witnesses' Testimony Falls Under Rule 602 and 701, Not Expert Testimony

A. Applicable Law

Lay witnesses may properly offer fact testimony and opinion testimony. Rule 602 of the Federal Rules of Evidence sets forth the well-established rule that a witness may testify as to matters within his or her personal knowledge. *See* Fed. R. Evid. 602. However, "personal knowledge of a fact 'is not an absolute' to Rule 602's foundational requirement, which 'may consist of what the witness thinks he knows from personal perception." *United States v. Cuti*, 720 F.3d 453, 458-49 (2d Cir. 2013) (citation omitted). Factual testimony under Rule 602, as the Second Circuit recognized, also encompasses "the fact of what [a witness] did not know and how, if [the witness] had known that independently established fact, it would have affected [the witness's] conduct or behavior." *Id.*

Rule 701 provides that opinion testimony from a lay witness is admissible if it is "(a) rationally based on the witness's perception; (b) helpful to clearly understanding the witness's testimony or determining a fact in issue; and (c) not based on scientific, technical, or other special knowledge within the scope of Rule 702." *See* Fed. R. Evid. 701. A "rational perception" is one that involves "first-hand knowledge or perception." *United States v. Yannotti*, 541 F.3d 112, 126 & n.8 (2d Cir. 2008) (citing *United States v. Rea*, 958 F.2d 1206, 1215 (2d Cir. 1992)). As to Rule 701(c), opinion testimony regarding technical subject-matter or which involves jargon or industry

terminology is not automatically rendered expert testimony under Rule 702.

Indeed, "some degree of specific-industry-related knowledge will not disqualify lay opinion testimony," as long as those opinions do "not depend on the sort of specialized training that scientific witnesses or statisticians rely upon when interpreting the results of their own experiments or investigations." *Yannotti*, 541 F.3d at 126. In other words, what matters is that the opinion "[results] from a process of reasoning familiar in everyday life," even if the testimony relates to complex matters. *Cuti*, 720 F.3d at 459 (upholding admission of lay testimony by sophisticated accountant and auditor with personal knowledge of events regarding accounting rules and treatment of allegedly fraudulent financial transactions as non-expert testimony); *see id.* at 460 (opinion testimony falls outside Rule 701 only when it is "based on specialized experience that the agent accumulated from other cases and involved a special reasoning process not readily understandable to the average juror," but is proper under Rule 701 when witnesses "testified based only on their experiences with matters pertinent to this case, and their reasoning was evident to the jury").

For example, an "owner or officer of a business" properly provides opinion testimony under Rule 701 regarding "the value or profits of the business" without being qualified as an expert because the opinion is based on "the particularized knowledge that the witness has by virtue of his or her position in the business," not the witness's "experience, training, or specialized knowledge within the realm of an expert." *Yannotti*, 541 F.3d at 125. Similarly, "a witness's specialized knowledge, or the fact that he was chosen to carry out an investigation because of this knowledge, does not render his testimony 'expert' as long as the testimony was based on his 'investigation and reflected his investigatory findings and conclusions, and was not rooted exclusively in his expertise.'" *Cuti*, 720 F.3d at 460 (citing *Bank of China, N.Y. Branch v. NBM LLC*, 359 F.3d 171,

181 (2d Cir. 2004)). In other words, Rule 701 permits witnesses "to testify to their personal perceptions in the form of inferences or conclusory opinions." *United States v. Garcia*, 413 F.3d 201, 211 (2d Cir. 2005).

B. The Anticipated Testimony by Victim-1, CW-1, and the Flashbots Representative Is Not Expert Testimony

The testimony that the Government expects to elicit from the Victim-1, CW-1, and the Flashbots Representative falls well within Rules 602 and 701: each of these witnesses will testify as to facts within their personal knowledge and matters that are rationally based on their own perception, squarely related to the issues in this case, with reasoning evident to the jury. For these reasons, none of their proposed testimony will be reliant on any specialized scientific or technical knowledge.

1. Victim-1

Victim-1's anticipated testimony regarding his MEV Bots' trading activity and why he used the MEV-Boost software are matters that rely directly and solely on Victim-1's own experience as a MEV-Boost user. Similarly, Victim-1's expected testimony regarding his discovery of the theft of cryptocurrency from his cryptocurrency wallet, his own investigation into how his cryptocurrency was taken, and his subsequent efforts to get his stolen cryptocurrency back are entirely reliant on his own conduct and perceptions. *See United States v. Rigas*, 490 F.3d 208, 224 (2d Cir. 2007) (explaining that "a witness's specialized knowledge . . . does not render his testimony 'expert' as long as it was based on his investigation and reflected his investigatory findings and conclusions, and was not rooted exclusively in his expertise"). These are all factual matters that were known to Victim-1 at the time of the events at issue based on his own experience as a victim of the Exploit, which are squarely proper under Rules 602 and 701.

Victim-1 can also properly explain his own understanding of any terms of art or jargon he

himself may use regarding his MEV Bots' trading activity and the MEV-Boost software based on his own experience as a trader who used MEV-Boost. Even if such testimony constitutes opinion testimony, it easily satisfies the requirements of Rule 701 because it is reliant on Victim-1's own experience as a trader and MEV-Boost user, because the jury cannot be expected to understand Victim-1's testimony without knowing the meaning of basic terms that Victim-1 may mention, and because it is the "product of reasoning processes familiar to the average person"—namely, picking up terms through experience engaging in some activity. Any average juror has similarly learned words and phrases from work, school, or other activities that he or she participates in. But that does not reflect reasoning dependent on specialized training or knowledge, and the defendants' arguments to the contrary would effectively bar lay witnesses in any case involving unfamiliar industries or activities from explaining the meaning of basic terms that they learn through experience. The Court should reject the defendants' arguments, which are plainly not the law. *United States v. Krikheli*, 461 F. App'x 7, 10 (2d Cir. 2012) (affirming admission of lay opinion testimony regarding industry terms of art by witness with lengthy experience in that industry); *United States v. Ferguson*, 676 F.3d 260, 294 & n.42 (2d Cir. 2011) (holding that testimony regarding meaning of jargon used by defendants was admissible based on witnesses' industry experience).

2. CW-1

At trial, CW-1 will testify about how the defendants planned the Exploit for months before executing it, how the defendants executed the Exploit just as they had planned it, and how the defendants subsequently concealed the Exploit by transferring the stolen cryptocurrency to the defendants' bank accounts through a series of on-chain and off-chain transfers. This type of testimony—which relies on CW-1's own participation in the conspiracy and not any specialized

scientific or technical training and experience—is quintessential fact witness testimony admissible under Rule 602. Such testimony is not expert opinion testimony subject to Rule 16(a)(1)(G), Rule 702, and *Daubert*, even if the witness were to offer some aspect of his opinion in the course of his testimony. *See Yannotti*, 541 F.3d at 126 (holding that "where a witness derives his opinion solely from insider perceptions of a conspiracy of which he was a member, he may share his perspective as to aspects of the scheme about which he has gained knowledge as a lay witness subject to Rule 701, not as an expert subject to Rule 702"); *see also United States v. Ghavmani*, 23 F. Supp. 3d 148, 171 (S.D.N.Y. 2014) (concluding that witness's testimony "concerning the complex financial transactions that were the subject of the conspiracies" was properly admitted under Rule 701, "in that it was based on his participation in the conspiracies").

As with Victim-1, CW-1 may also properly explain CW-1's own understanding of certain terms of art relating to the use of MEV-Boost, which is "based on his day-to-day participation in the conspirac[y], not on specialized knowledge." *Ghavmani*, 23 F. Supp. 3d at 172. In other words, it is simply not the law that any lay testimony that touches upon an unfamiliar or specialized subject must be qualified under Rule 702 and *Daubert*. Indeed, the Second Circuit acknowledged that the loansharking activity at issue in *Yannotti* may not be "an activity about which the average person has knowledge," but nonetheless allowed lay opinion that the witness "reached from his own loansharking experience derived from a reasoning process familiar to average persons," and not "the sort of specialized training that scientific witnesses or statisticians rely upon when interpreting the results of their own experiments or investigations." *Yannotti*, 541 F.3d at 126. And in *Rigas*, the Second Circuit allowed extensive testimony about accounting concepts from a lay witness. *Rigas*, 490 F.3d at 225; *accord Cuti*, 720 F.3d at 458-60 (holding that accountants who were "personally familiar with the accounting of the transactions at issue" could testify

regarding the effect of the fraud on the accounting treatment of those transactions without rendering expert testimony).

3. The Flashbots Representative

The Flashbots Representative is expected to describe how the MEV-Boost software was exploited by the perpetrators of the Exploit; his direct participation in Flashbots' efforts to determine the nature of the exploit and how it occurred; why this exploit mattered to MEV-Boost (namely, that it undermined the very purpose of the MEV-Boost software and the issues that MEV-Boost was designed to address for its users); and the Flashbots Representative's efforts to remediate the Exploit, including the Flashbot Representative's actual participation in communications with the perpetrators of the Exploit after the Exploit occurred. Thus, there is no reasonable dispute that all of this anticipated testimony is within the Flashbots Representative's personal knowledge and will be based on the Flashbots Representatives' rational perception of events. *See Yannotti*, 541 F.3d at 125-26.

Similarly, the Flashbots Representative's anticipated testimony is undoubtedly helpful to the jury. Indeed, the Flashbots Representative's testimony regarding how the Flashbots Representative designed the MEV-Boost software to work and how Flashbots publicized MEV-Boost's features—including the roles and designed interactions between the block builder, the validator, and the relay—is necessary background for the jury to understand why the defendants' conduct was fraudulent. *Accord Garcia*, 413 F.3d at 214 (explaining that hypothetical testimony by undercover officer regarding his "direct dealings with a group of persons" and "opinion as to what the words and actions witnessed conveyed about the relative relationships of the participants" "helps the jury gain 'an accurate reproduction of the event' actually witnessed by the agent" (citation omitted)). And by extension, the Flashbots Representative's basic factual explanation of

terms relating to Ethereum, MEV-Boost, and who the different MEV-Boost participants are is similarly necessary to understanding the Flashbots Representative's testimony. *Accord Yannotti*, 541 F.3d at 126 (concluding that lay opinion testimony was "helpful to the jury" where it interpreted the meaning of certain words and references used in the course of loansharking business); *see also Krikheli*, 461 F. App'x at 10; *Ferguson*, 676 F.3d at 294 & n.42.

Moreover, the Flashbots Representative's expected testimony regarding the MEV-Boost software is not based on opinions rendered from any scientific, specialized, or technical knowledge, but rather based on his actual, direct experience as the Flashbots product lead who oversaw the development, testing, and implementation of the very software that the defendants exploited. There is no material difference between a product developer providing percipient testimony about a product that he developed and, for example, (i) a prison employee testifying about the policies and procedures of a prison based on the employee's "personal knowledge of such policies and practices through his everyday experiences as an employee there," *Johnson v. Barney*, 360 F. App'x 199, 201-02 (2d Cir. 2010); (ii) the owner of a business testifying about the value or profits of the business based on "the particularized knowledge that the witness has by virtue of his or her position in the business," *Yannotti*, 541 F.3d at 125; or (iii) an employee of a company testifying about the company's finances and financial statements, including the effect that the defendants' reclassifications of financial transactions had on certain entities owned by the defendants, based on the employee's "observations during his twenty months as [a company] employee," through which he "was well-acquainted with the records of [the company] and [the defendants' entities]" because he "was responsible for correcting [the company's] financial

statements,"[4] *Rigas*, 490 F.3d at 223-25.

Simply put, there is nothing improper about a product developer offering percipient testimony—whether fact testimony or lay opinion testimony—regarding the design and function of a product that he personally worked on and oversaw in the course of his employment as a product developer. Judge Failla's reasoning in *523 IP LLC v. CureMD.Com*, 48 F. Supp. 3d 600 (S.D.N.Y. 2014), is on point. There, two co-founders of CureMD were "involved in the development of CureMD's [computer] system since its inception" and "assisted in the conception, design, and writing of the source code" for that system. *Id.* at 635. Judge Failla concluded that the co-founders could testify under Rule 701 to their "deep personal knowledge of the CureMD system, its features, and functionality." *Id.* So, too, here. The anticipated testimony of the Flashbots Representative—who was involved in developing, testing, and implementing MEV-Boost from its inception—regarding MEV-Boost's architecture, features, and functionality is also "well within the purview of an opinion rationally based on the witness's perception." *Id.* (cleaned up); *see also Medforms, Inc. v. Healthcare Mgmt. Solutions, Inc.*, 290 F.3d 98, 110-11 (2d Cir. 2002) (testimony by computer programmer's supervisor regarding significance of programmer's work on two computer programs and regarding meaning of "program" were properly admitted under Rule 701 because his "opinions were rationally based on his perceptions as [the programmer's supervisor]" and "his everyday experience as a computer programmer and specifically on his work on [the two computer programs]"); *Bic Corp. v. Far Eastern Source Corp.*, 23 F. App'x 36, 39 (2d Cir. 2001) (affirming admission of lay opinion testimony regarding a

[4] In *Rigas*, another company employee, who was a co-conspirator of the defendants, also testified regarding the sham purpose and effect of the reclassifications. *Rigas*, 490 F.3d at 232. The defendants did not contend on appeal that this testimony should have been subject to any expert disclosures or the gatekeeping requirements of Rule 702.

consumer survey by a witness who "had worked directly on the design and interpretation of the survey"); *accord B&G Plastics, Inc. v. E. Creative Indus., Inc.*, 98 Civ. 0884, 2004 WL 307276, at *8 (S.D.N.Y. Feb. 18, 2024) (explaining that "[c]ourts have permitted lay witnesses to testify under Rule 701 to their opinions when those opinions are based on a combination of their personal observations of the incident in question and background information they acquired through earlier personal observations" (citing *Securitron Magnalock Corp. v. Schnabolk*, 65 F.3d 256, 265 (2d Cir. 1995)).

Again, the fact that the average person may not be acquainted with cryptocurrency trading does not, as the defendants assert, transform every witness in a cryptocurrency case into an expert subject to Rule 702. That is precisely what *Yannotti* instructed in permitting lay opinion about loansharking derived from experience, even if loansharking is not "an activity about which the average person has knowledge." *Yannotti*, 541 F.3d at 126. For the same reasons, the Flashbots Representative's expected testimony about his own experience identifying and responding to the Exploit, and the basic context of the MEV-Boost software necessary to understand those facts is proper under Rules 602 and 701 precisely because it arises from the Flashbots Representative's personal experience as the product lead for MEV-Boost. *Accord B&G Plastics*, 2004 WL 307276, at *7 (finding testimony by company president, who was "involved in the design, manufacture, and marketing" of a particular product, properly admitted under Rule 701 because the witness's opinions regarding his "perception of the benefits of certain design modifications as well as observations he has made" about the market were based on his own "observations of the [product] at issue and background information he acquired about the industry from his experience").

* * *

Taken to its logical conclusion, the defendants' argument that *any* testimony about

technical or complex subject matter—even by witnesses with personal knowledge—is subject to the gatekeeping requirements of *Daubert* and Rule 702 means that, should the defendants choose to testify in their own defense, the defendants' own testimony regarding the Exploit would be subject to these evidentiary strictures as well. *See Taylor v. Illinois*, 484 U.S. 400, 410 (1988) ("The accused does not have an unfettered right to offer testimony that is incompetent, privileged, or otherwise inadmissible under standard rules of evidence."). Of course, this cannot be—and is not—the rule, because whether any given testimony falls within the purview of Rule 701 or Rule 702 turns on whether it results from *reasoning processes* familiar to the average person. A product manager's knowledge about a product he helped develop, a victim's knowledge about a product that he used, and a co-conspirator's knowledge about a fraud scheme in which he participated all rely on reasoning processes that are "straightforward and transparent," even if the subject matter was "technical and unfamiliar to everyday life." *See Cuti*, 720 F.3d at 458-60.

The cases that the defendants cite are not to the contrary. In *Bank of China*, cited extensively in the defendants' brief, the Second Circuit found it improper under Rule 701 to admit certain opinion testimony about "the business community's understand[ing]" of certain things, how things typically "work[] in the context of an international commercial transaction," and the circumstances in which certain transactions are "considered fraud," to the extent that the testimony was "not based entirely on [the witness's] perceptions," but on his "experience and specialized knowledge in international banking." *Id.* at 180-82. Unlike *Bank of China*, the Government's percipient witnesses will not providing any general opinions about the cryptocurrency industry; instead, as discussed above, their testimony will be based on matters they personally did or observed. Moreover, *Bank of China* does not stand for the broad proposition that nobody in a specialized industry can testify regarding terms used in that industry—it simply applies the

principle that lay opinion testimony must be based on a witness's perception.

Likewise, the Second Circuit's decision in *Garcia* is readily distinguishable: the *Garcia* court concluded that testimony from a law enforcement agent that the defendant was a partner in the charged narcotics distribution conspiracy was improper lay opinion testimony because it was "he was expressing an opinion informed by all the evidence gleaned by various agents in the course of the investigation and not limiting himself to his own personal perceptions." *United States v. Garcia*, 413 F.3d 201, 213 (2d Cir. 2005).[5] Here, as explained above, the expected testimony by Victim-1, CW-1, and the Flashbots Representative relies on their own "experiences with matters pertinent to this case." *Id.* Fundamentally, the defendants cite no case for their extraordinary notion that a victim-witness, a cooperating witness, and a percipient fact witness must be noticed as experts pursuant to Rule 16(a)(1)(G), and subject to the related gatekeeping requirements of Rule 702 and *Daubert*. Their argument should be rejected. The defendants' reliance on *United States v. Cabrera*, 13 F.4th 140 (2d Cir. 2021) is misplaced for similar reasons. There, a DEA agent opined that the defendant was an "experienced" drug dealer compared to the "average drug dealer" because the defendant deployed certain countersurveillance techniques that an average drug dealer would not know about,[6] from which the agent concluded that the defendants "was experienced to know that he knows some of our law enforcement techniques." *Id.* at 149-50. The

[5] Notably, the *Garcia* court made clear that testimony of this nature from a law enforcement witness would be improper whether it was lay or expert testimony. *United States v. Garcia*, 413 F.3d 201, 210 (2d Cir. 2005).

[6] Of note, the defendant did not challenge the agent's definition of "countersurveillance." *See Cabrera*, 13 F.4th at 149 (noting that the defendant "does not challenge that (seemingly unobjectionable) testimony"). This is unsurprising because, as the Government explained above, a witness can explain the meaning of terms that the witness learns through personal experience in some industry.

Second Circuit explained that this conclusion was based on the agent's "specialized knowledge and experience as a DEA detective to infer that [the defendant] was more experienced than your average drug dealer," as opposed to "relat[ing] events, or describ[ing] [the defendant's] atypical driving patterns, or contextualiz[ing] the relationship between the defendant with a co-conspirator." *Id.* Here, relating events, describing what Victim-1, CW-1, and the Flashbots Representative perceived, and explaining terms that will aid the jury in understanding those events and perceptions is exactly what Victim-1, CW-1, and the Flashbots Representative are expected to do. There is no legal basis to subject such testimony to the gatekeeping requirements of *Daubert* and Rule 702.[7]

[7] The out-of-Circuit authority the defendants cite for the overbroad proposition that courts "regularly" find that "technical testimony by percipient witnesses falls under Rule 702" fares no better. (Mot. at 10). Again, the technical subject matter of the testimony is not what matters; the technical reasoning is what matters. Thus, for example, *United States v. Figueroa-Lopez*, 125 F.3d 1241 (9th Cir. 1997) is inapposite because the Ninth Circuit—like the Second Circuit in *Cabrera*—concluded that a DEA agent's conclusion that a drug dealer's behavior was consistent with being an "*experienced* drug trafficker" relied on "demonstrable expertise" and was explicitly based on the agent's "training and experience." *Id.* at 1246. Similarly, *United States v. Ramirez*, 491 F. App'x 65 (11th Cir. 2012), is distinguishable: there, the court found a medical lab technician's opinion that the defendant likely manipulated blood samples using a centrifuge to be improper lay opinion testimony because the *reasoning* process "that the white blood cell count of blood can be manipulated by separating the blood into different layers in a centrifuge" relied upon "scientific, technical, or other specialized knowledge." *Id.* at 73-74. Here, by contrast, there is no leap of reasoning that is similarly reliant on specialized knowledge or training. Finally, *In re: Taxotere (Docetaxel) Products Liability Litigation*, 26 F.4th 256 (5th Cir. 2022) is even less applicable. In that case, a witness provided his interpretation and analysis of clinical trial datasets as a board-certified oncologist, opining on whether those datasets showed the resolution of alopecia after chemotherapy. *Id.* at 266-67. Unlike any of the testimony that Victim-1, CW-1, or the Flashbots Representative are expected to offer, the oncologist's interpretation and analysis of medical data in *Taxotere* is plainly the "product of 'scientific, technical, or other specialized knowledge'" resulting from the "application of scientific 'principles and methods.'" *Id.* at 267.

C. The Defendants' Reliance on *Eisenberg* and *Storm* Is Misplaced

In support of their Motion, the defendants inaccurately claim that the Government's position with respect to the Flashbots Representative, Victim-1, and CW-1 in this case is "at odds" with the Government's disclosure of experts in *United States v. Eisenberg*, No. 23 Cr. 10 (AS) (S.D.N.Y.), and *United States v. Storm*, No. 23 Cr. 430 (KPF) (S.D.N.Y.). (Motion, at 13-14). It is not. As a threshold matter, the defendants do not cite—because there is none—any legal authority for their implicit proposition that the Government is required to use expert testimony in cases involving technical complexity. Furthermore, to the extent that the *Eisenberg* and *Storm* cases have any relevance to this Motion, those cases support the Government's position here. Unlike Victim-1, CW-1, and the Flashbots Representative, the experts noticed in *Eisenberg* and *Storm* were not percipient witnesses. That the Government made the strategic decision to notice industry cryptocurrency experts in *Eisenberg* and *Storm*, therefore, has no bearing on the Court's decision on this Motion. In addition, in both *Eisenberg* and *Storm*, the Government called percipient witnesses who testified on highly technical matters. *United States v. Eisenberg*, 23 Cr. 10 (AS), Dkt. 158 (S.D.N.Y Apr. 8, 2023) (presenting lay testimony of Brian Smith, a "contributor" to and user of the Mango Markets platform, on how Mango Markets was used and relevant terminology); *United States v. Storm*, No. 23 Cr. 430 (KPF) (S.D.N.Y. Jul. 16, 2025), Trial Tr. 205-08 (testimony of Justin Bram explaining cryptocurrency concepts, including smart contracts, mixers, and high-yield staking), Trial Tr. 291-300 (testimony of Andrew Llacuna, explaining non-fungible tokens); *see also United States v. Guo*, 23 Cr. 118 (AT) (S.D.N.Y. June 13, 2024), Trial Tr. 2385-87 (permitting testimony about how lay witness's understanding of "the design and function" of a purported crypto exchange and its purported digital assets informed his business recommendations).*United States v. Sam Bankman-Fried*, 22 Cr. 673 (LAK), Dkts. 356,

366 (S.D.N.Y. Oct. 5, 2023) (cooperating witness testimony of Gary Wang and Nishad Singh regarding computer code); *United States v. Cuomo*, 125 F.4th 354, 364–65 (2d Cir. 2025) (describing a lay witness's testimony regarding how a particular computer code functioned).

II. The Court Should Order Defendants to Make Their Expert Disclosures Promptly

The defendants claim that, absent the requested disclosures, they "cannot be expected to be prepared to respond to the government's case" because "neither the Indictment nor the government's disclosures to date identify the protocols and expectations that the Peraire-Buenos are alleged to have thwarted in this novel and complex case." (Mot. at 16). The defendants are wrong both as a legal matter and as a factual matter. To start, there is no basis in the Constitution or Rule 16—and the defendants articulate none—for the proposition that a defendant cannot "decide what expert testimony he intended to rely upon at trial without any knowledge of the government's case." *United States v. Finazzo*, 10 Cr. 457 (RRM), 2013 WL 618425, at *2 (E.D.N.Y. Feb. 19, 2013); *see United States v. Rajaratnam*, S2 09 Cr. 1184 (RJH), 2011 WL 723530, at *5 (S.D.N.Y. Feb. 25, 2011) (rejecting argument that "disclosure is not required because 'the defense simply does not know what expert testimony it "intends to use" in its case-in-chief because the government's case remains unfixed and unpredictable'" (citation omitted)). Indeed, "a defendant would always like more information about the government's case before revealing anything about his or her own, but Rule 16 conditions a defendant's disclosure obligations on the government's having made certain specified disclosures, not on the government's laying open its entire case [to] the defendant's satisfaction." *Rajaratnam*, 2011 WL 723530, at *5. Accordingly, the Court should reject the defendants' attempts to skirt their disclosure obligations by claiming that they "lack[] sufficient information about the government's case to decide whether [they] will in fact call an expert." *Id.*

In any event, as the Court knows, Government's allegations regarding the defendants' crimes, including their technical execution, have been extensively articulated in the Indictment, in search warrant affidavits, in briefs to the Court, and at two oral arguments. Those theories are backed by the extensive discovery in this case, which contains material responsive to the overlapping categories of technical information that the defendants claim they need to notice experts for their case-in-chief. For example, the Google Search Warrant Affidavit—on which the Government relied for the "explication of the software the government describe at length in oral argument on June 17"—was produced in Rule 16 discovery, contains information obtained from interviews of Victim-1 and the Flashbots Representative, and is responsive to all categories of information that the defendants claim they need to notice their own experts. (*See* Dkt. 105 at 2; Mot. at 1). The defendants' Slack messages, too, contain information responsive to these categories, including the Slack message identified in Part B of the Relevant Background section, *supra*, in which Anton Peraire-Bueno explains the MEV-Boost system and the role of various participants in that system. With respect to "how the various computer programs operated in the transactions at issue," the Rule 16 discovery includes the computer code that the defendants wrote to execute the Exploit. In addition, the Rule 16 discovery contains the defendants' search history, including Anton Peraire-Bueno's Google search for the public code repository that contained the MEV-Boost software that was exploited, and so the defendants cannot claim any lack of notice based on not knowing how the MEV-Boost software operated at the time of the Exploit. Furthermore, Flashbots' publicly available website contains descriptions of the MEV-Boost system, including the roles, functions, and obligations of participants in the MEV-Boost system, and the purpose that MEV-Boost serves on the Ethereum network. As shown in Exhibit D, under the MEV-Boost system, validators no longer have a role to "build[] the best block from all

available transactions" and instead are limited to "proposal duties only," whereby the validator "[r]eceive[s] an execution payload header from one or more relays and blindly sign[s] a block without seeing the underlying execution payload (i.e. the blinded TXs escrowed by the relay)." These are not matters of expert opinion or "interpretation" as the defendants' claim: these are the facts that Flashbots itself told the public and its users about its own services. In light of these disclosures—and many others—the defendants have all that they need to notice an expert, should they choose to use one in their case-in-chief.

The defendants' reliance on Rule 16 of the Federal Rules of Criminal Procedure is also misplaced. (Mot. at 16). The defendants frame their disclosure obligations as "responsive" (Dkt. 105, at 2), but this is not an accurate reflection of Rule 16, which on its face does not cabin a defendant's expert disclosures to those that are "responsive" to the Government's expert disclosures. *See* Fed. R. Crim. P. 16(a)(1)(G) & 16(b)(1)(C) (requiring the Government and defendant to make expert disclosures "sufficiently before trial to provide a fair opportunity" for its adversary "to meet [its] evidence"). The defendants have argued that their expert disclosure obligations "only apply after the government has complied with its disclosure obligations," citing Federal Rule of Criminal Procedure 16(b)(1)(C). (*See* Dkt. 45, at 3; Mot. at 16). But the Government *has* complied with its disclosure obligations—it disclosed the expert testimony that it intends to elicit at trial. *Finazzo*, 2013 WL 618425, at *2 (concluding that "comply" within the meaning of Rule 16(b)(1)(C) means "*either* that the government fully discloses its expert testimony *or* that it represents that it has no experts" (emphasis in original)); *cf. Rajaratnam*, 2011 WL 723530, at *2-3 (rejecting defense argument that the defendant was absolved of its expert disclosure obligations based on the Government's statement that it did not intend to introduce any expert testimony at trial). Now the defendant must promptly do so, consistent with the Court's

original order setting a deadline for the defense's expert disclosures. Such disclosure must be made by the defense "sufficiently before trial to provide a fair opportunity for the government to meet the defendant's evidence." Fed. R. Crim. P. 16(b)(1)(C)(ii).

To be sure, the Government may elect not to use expert testimony at all in its case-in-chief, and a defendant can still choose to notice several experts that they might call in their defense. *See, e.g.*, *United States v. Charlie Javice and Olivier Amar*, 23 Cr. 251 (AKH) (S.D.N.Y. 2024) (the Government noticed no experts, while the two defendants collectively noticed six). Similarly, it is not uncommon for the Government and the defense to provide notice of expert testimony regarding different, unrelated topics.[8] In either scenario, it is simply "not the case that requiring [a defendant] to disclose his intent regarding expert witnesses would unfairly compel him to reveal his cards while the government keeps its hand close to the chest" by not disclosing any experts, or by disclosing experts on the same topics as the defendant. *Rajaratnam*, 2011 WL 723530, at *3. What Rule 16 "requires [is] reciprocity; it makes no provision for a holistic comparison of what each side has or has not disclosed." *Id.* at *5. A defendant's "obligation to make expert disclosures does not turn on whether the government will call a certain witness," but rather "on whether the government has made its own expert disclosures." *Id.* The Government has done so here, and the Court should require the defendants to promptly provide the requisite disclosures under Rule 16(b)(1)(C) for any experts that they intend to call in their case-in-chief, sufficiently in advance of

[8] Consider, for example, a bank robbery case in which the Government provides notice of a cellsite location expert to establish the defendant's presence at the bank, and the defendant provides notice of a handwriting expert to show that the defendant did not author the demand note. Having disclosed its experts, the Government would still be in compliance with its obligations, and the fact that the defendant's handwriting expert may not be "responsive" to the Government's cellsite location expert does not absolve the defense of its obligation to provide notice of the experts it intends to call in its case-in-chief.

any deadline set for the Government to make rebuttal expert disclosures (currently scheduled for August 1, 2025) and to file motions *in limine* and *Daubert* motions (currently scheduled for August 22, 2025). (*See* Dkt. 46).

CONCLUSION

For the reasons set forth above, the defendants' Motion to Compel should be denied, and the Court should order the defendants to promptly notice any experts they intend to call in the defense case at trial.

Respectfully submitted,

JAY CLAYTON
United States Attorney

By: /s/ *Rushmi Bhaskaran*
Rushmi Bhaskaran
Jerry Fang
Danielle Kudla
Assistant United States Attorneys
212-637-2439 / 2584 / 2304

Dated: July 17, 2025
New York, New York